[redacted]

FD-1036 (Rev. 10-16-2009)

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: EMAIL **Date:** 08/03/2017

Title: (U) [redacted] [redacted]

(U)

Approved By: SSA [redacted]

b3
b6
b7C
b7E

Drafted By: [redacted]

Case ID #: [redacted] ~~(S)~~ [redacted] [redacted]

(U)

[redacted] ~~(S//NF)~~ [redacted] [redacted]

[redacted]

~~Reason: 1.4(b)~~
~~Derived From: FBI NSISC-20090615~~
~~Declassify On: 20421231~~

♦♦

~~SECRET//NOFORN~~

7/27 articles:

- What's next in Congress for the Pentagon Kaspersky Software Ban
- Ransomware 'here to stay', warns Google study
- Report: Russia used fake Facebook accounts to target Macron campaign
- The biggest threat to cybersecurity is not enough info sharing
- Radiation monitoring systems rife with security flaws
- DOJ indicts Russian for alleged $4 billion laundering operation

7/28 articles:

- Iranian Hackers Used Female 'Honey Pot' To Lure Targets: Researchers
- Hackers copying WannaCry and Petya ransomware tricks
- Symantec distrust to begin in Chrome from April 2018
- Report: SEC must improve how it protects against cyber attacks
- North Korea hackers 'want cash not secrets'
- Every iOS user should update to 10.3.3 now to avoid this Wi-Fi hack
- How one small hack turned a secure ATM into a cash-spitting monster
- Android spyware can record your voice, take photos with your camera, and steal app data
- Report goes in-depth on power grid cyber vulnerabilities and why they won't be fixed soon
- Lawyer's 'Inadvertent' E-Discovery Failures Led to Wells Fargo Data Breach
- 400,000 UniCredit Accounts Hacked, Data Exposed
- Google: Ransomware victims shelled out $25 million over the last two years
- Virgin America says a hacker broke into its network, forced staff to change passwords

7/31 articles:

- Putin passes law that will ban VPNs in Russia
- WikiLeaks releases Macron French presidential campaign emails
- Apple kowtows to China, pulls some VPN apps from Chinese App Store
- Hackers breach dozens of voting machines brought to conference
- House panel asks agencies for Kaspersky docs
- Hacking group ShadowBrokers raises prices for leaks
- Phishers steal Chrome extension from developer
- Seagate to pay millions for forking over employee info to scammers
- Researchers remotely hack Tesla Model X
- Hackable smart car wash systems can hurt people
- Employees working while on holiday open orgs to security risks
- Ransomware Attack Affects 300,000 Patients of Women's Clinic

8/1 articles:

- Hackers Break Into HBO's Computer Networks, May Have Leaked 'Game of Thrones'
- Facebook shuts down robots after they invent their own language
- WikiLeaks publishes searchable archive of Emmanuel Macron's campaign emails
- FCC says its cybersecurity measures to prevent DDoS attacks must remain secret

b6
b7C

[redacted]

[redacted]

This Issue's News Articles:

- What's next in Congress for the Pentagon Kaspersky Software Ban
- Ransomware 'here to stay', warns Google study
- Report: Russia used fake Facebook accounts to target Macron campaign
- The biggest threat to cybersecurity is not enough info sharing
- Radiation monitoring systems rife with security flaws
- DOJ indicts Russian for alleged $4 billion laundering operation

b6
b7C
b7E

What's next in Congress for the Pentagon Kaspersky Software Ban

Politico, 26 Jul 2017: While it could be months before House and Senate lawmakers agree on a final defense policy bill, they are expressing confidence that the finished measure will contain some form of an amendment to bar the Pentagon from using software developed by Moscow-based cyber giant Kaspersky Lab. Now that the Senate draft of the measure — the fiscal year 2018 National Defense Authorization Act — has been queued for floor time, both chambers will soon be looking to hammer out differences between their separate versions, including the Senate bill provision that would block the use of Kaspersky software on DoD networks and require the Pentagon to "immediately" sever any DoD-connected systems that are "using" Kaspersky technology. The House-passed NDAA doesn't include such language, but lawmakers in both chambers told POLITICO that they expect some version of the Senate clause to make it into the blended legislation, despite some reservations. "I think it's a matter of which one of us has the best idea," said Sen. Mike Rounds, who chairs the Senate Armed Services Cybersecurity Subcommittee. A Kaspersky ban would serve as another piece of legislation meant to thwart Russian hacking — a cause both parties have taken up as many lawmakers chastise the White House for not doing enough in the wake of last year's alleged Russian election interference campaign. The Moscow-based company is one of the world's largest cyber firms, claiming over 400 million global users, and the fear is that its wide reach gives Russia a backdoor into key American networks. Kaspersky strenuously denies any ties to the Russian government and has offered up its source code for inspection. Several potential roadblocks stand in the way of lawmakers reaching consensus on a Kaspersky ban. Russian officials have suggested they may strike back at the U.S. if it enacts a ban. Meanwhile, the Senate provision's language is "problematic," said a House Armed Services Committee aide, because it could prove too difficult to implement. Still, while the language may not appear verbatim in the final authorization bill, some form of it seems destined to make the final cut. "There are public reports that are showing Kaspersky has a relationship with the Russian government that has given a lot of people pause," according to Sen. Jack Reed, the top Democrat on SASC. "It's a serious issue."

Ransomware 'here to stay', warns Google study

BBC, 27 Jul 2017: Cyber-thieves have made at least $25m (£19m) from ransomware in the last two years, suggests research by Google. The search giant created thousands of virtual victims of ransomware to expose the payment ecosystem surrounding the malware type. Most of the money was made in 2016 as gangs realized how lucrative it was, revealed a talk at Black Hat. Two types of ransomware made most of the money, it said, but other variants are starting to emerge. "It's become a very, very profitable market and is here to stay," said Elie Bursztein from Google who, along with colleagues Kylie McRoberts and Luca Invernizzi, carried out the research. Ransomware is malicious software that infects a machine and then encrypts or scrambles files so they can no longer be used or read. The files are only decrypted when a victim pays a ransom. Payments typically have to be made using the Bitcoin virtual currency. Mr Bursztein said Google used several different methods to work out how much cash was flowing towards ransomware creators. As well as drawing on reports from people who had paid a ransom, it sought out the files used to infect machines and then ran those on lots of virtual machines to generate "synthetic victims", he said. It then monitored the network traffic generated by these victims to work out to where money would be transferred. The data gathered in this stage was also used to find more variants of ransomware and the 300,000 files it found broke down into 34 of them, he said. The most popular strains were the Locky and Cerber families, added Mr Bursztein. Payment analysis of the Bitcoin blockchain, which logs all transactions made using the e-currency, revealed that those two strains also made the most money over the last year, he said, with Locky collecting about $7.8million and Cerber $6.9million. The research project also revealed where the cash flowed and accumulated in the Bitcoin network and where it was converted back into cash. More than 95% of Bitcoin payments for ransomware were cashed out via Russia's BTC-e exchange, found Google. On 26 July, one of the founders of BTC-e, Alexander Vinnik, was arrested by Greek police on money laundering charges. The police were acting on a US warrant and his extradition to America is being sought. The gangs behind the ransomware explosion were not likely to stop soon, said Mr Bursztein, although established strains are facing competition from newer ones. "Ransomware is a fast-moving market," he said. "There's aggressive competition coming from variants such as SamSam and Spora." Novel variants were expanding quickly and many were encouraging fast expansion by paying affiliates more if they placed the malware on to large numbers of machines. The ransomware as a service model was already proving popular, he warned. "It's no longer a game reserved for tech-savvy criminals," he said. "It's for almost anyone."

Report: Russia used fake Facebook accounts to target Macron campaign

Fox News, 27 Jul 2017: Russia used fake Facebook accounts to try to access personal data on associates of candidate Emmanuel Macron during France's 2017 presidential election, a report says. Citing unnamed sources, Reuters reported a total of 12 bogus Facebook accounts were created, in the names of friends of members of the Macron camp, in a bid to spy on the election's eventual winner, the report said. Reuters said it received the information from an unnamed U.S. congressman and two other people who were briefed on the matter. Although Russia has continued to deny allegations of election meddling, U.S. intelligence agencies confirmed Russia's involvement in a May conversation with Reuters. However, those intelligence officials could not verify that the Kremlin was behind the hacking. Facebook employees became aware of spying during the first round of the French election, and the social networking company confirmed to Reuters the presence of bogus accounts in France that were subsequently deactivated and deleted. It is not believed the hackers were able to give away any personal information or download malicious software. However, Macron campaign officials had content of their emails leaked online in the final days of the runoff portion of the election. A unit of the Russian intelligence agency GRU -- the same group believed to be behind U.S. election meddling -- is believed responsible for the effort targeting Macron's campaign, Reuters reported. The news

Facebook shuts down robots after they invent their own language

The Telegraph, 1 Aug 2017: Facebook shut down a pair of its artificial intelligence robots after they invented their own, creepy language. Researchers at Facebook Artificial Intelligence Research built a chatbot earlier this year that was meant to learn how to negotiate by mimicking human trading and bartering. But when the social network paired two of the programs, nicknamed Alice and Bob, to trade against each other, they started to learn their own bizarre form of communication. The chatbot conversation "led to divergence from human language as the agents developed their own language for negotiating," the researchers said. The two bots were supposed to be learning to trade balls, hats and books, assigning value to the objects then bartering them between each other. But since Facebook's team assigned no reward for conducting the trades in English, the chatbots quickly developed their own terms for deals. "There was no reward to sticking to English language," Dhruv Batra, Facebook researcher, told FastCo. "Agents will drift off understandable language and invent codewords for themselves. "Like if I say 'the' five times, you interpret that to mean I want five copies of this item. This isn't so different from the way communities of humans create shorthands." Facebook said when the chatbots conversed with humans most people did not realize they were speaking to an AI rather than a real person. The researchers said it wasn't possible for humans to crack the AI language and translate it back into English. "It's important to remember, there aren't bilingual speakers of AI and human languages," said Batra.

WikiLeaks publishes searchable archive of Emmanuel Macron's campaign emails

Reuters, 1 Aug 2017: WikiLeaks said on Monday it had published a searchable archive of more than 21,000 verified emails associated with key figures in the election campaign of President Emmanuel Macron. The stolen data was originally dumped on the internet in May, on the eve of the French presidential run-off between Macron and far-right opponent Marine Le Pen, in an apparent attempt to undermine voters' confidence. Within hours of the leak, Macron's staff alleged it had been targeted by a "massive and coordinated" hacking operation. The document dump came too late in the campaign to have any direct influence on the election, in part because the country's electoral commission warned it was a crime to republish any details from the emails before the balloting. French newspapers who have poured over the documents since then said they had found nothing scandalous to report. By turning the dump into a database, WikiLeaks has made the documents easily searchable for anyone with a web browser. The cyber attack drew comparisons with the 2016 U.S. election campaign, during which U.S. intelligence agencies alleged Russia had interfered to benefit President Donald Trump. Russia denies meddling in the U.S. election. Macron's team also blamed Russian interests in part for earlier attempts to interfere with their campaign. The Kremlin has denied it was behind any such attacks. At the time, WikiLeaks did not publish the Macron documents themselves, but said they were doing so now after attempting to verify the authenticity of the email addresses. WikiLeaks did not say how the emails were obtained. In its statement, it sought to cast doubt on the theory that Russia was behind the attack, citing a comment by a French government cyber security official that the document dump appeared to be the work of an "isolated individual". WikiLeaks said it found 21,075 verified emails in an archive of 71,848 emails, along with 26,506 attached documents, which it also published. They spanned the eight years between March 2009 and April 2017, the month of the first round of the French election.

FCC says its cybersecurity measures to prevent DDoS attacks must remain secret

TechCrunch, 31 Jul 2017: The FCC has provided a few — very few — details of the steps it has taken to prevent attacks like the one that briefly took down its comment system in May. The agency has faced criticism over its secrecy regarding the event, and shows no sign of opening up; citing "the ongoing nature of the threats," to reveal its countermeasures would "undermine our system's security." These cryptic comments are the first

b6
b7C

[redacted]

[redacted]

This Issue's News Articles:

- Putin passes law that will ban VPNs in Russia
- WikiLeaks releases Macron French presidential campaign emails
- Apple kowtows to China, pulls some VPN apps from Chinese App Store
- Hackers breach dozens of voting machines brought to conference
- House panel asks agencies for Kaspersky docs
- Hacking group ShadowBrokers raises prices for leaks
- Phishers steal Chrome extension from developer
- Seagate to pay millions for forking over employee info to scammers
- Researchers remotely hack Tesla Model X
- Hackable smart car wash systems can hurt people
- Employees working while on holiday open orgs to security risks
- Ransomware Attack Affects 300,000 Patients of Women's Clinic

b6
b7C
b7E

Putin passes law that will ban VPNs in Russia

TechCrunch, 30 Jul 2017: Russia has banned VPNs and other technology that allows users to gain anonymous access to websites. The new law (link), signed today by President Vladimir Putin, goes into effect on Nov. 1 and represents another major blow to an open Internet. This weekend, news broke that Apple has removed most major VPN apps from the App Store in China to comply with regulations passed earlier this year that require VPN apps to be explicitly licensed by the Chinese government. According to state-run news agency RIA (link), Leonid Levin, chairman of the Duma's committee on information policy and technology, has said that the law is not targeted at "introducing new bans for law-abiding citizens." Instead, he claims it is to prohibit access to illegal content. The scope of what is considered "illegal content" in Russia, however, has widened considerably during Putin's third term as president, with the government exerting more control over what people access or post online. As Freedom House notes, "anti-extremism laws are widely used as a pretext to block political content, often without judicial oversight." Russia's attempts to limit access to online information are concurrent with legislation that may put the privacy of users at risk. In 2015, the government passed legislation that requires all user data from Russian citizens to be stored in Russian-based servers, and last year it passed another law that requires telecoms and Internet service providers to retain traffic data for up to a year, a move that prompted VPN provider Private Internet Access to discontinue its Russian gateways.

b7E

WikiLeaks releases Macron French presidential campaign emails

Fox News, 31 Jul 2017: WikiLeaks on Monday released a searchable database stocked with more than 21,000 "verified" emails that the anti-secrecy site claimed originated with the campaign of French president Emmanuel Macron. Wikileaks stated nearly 72,000 emails, including 26,506 attachments, were also released to provide context. However, the organization cautioned only "21,075 emails have been individually forensically verified" through its Domain Keys Identified Mail system. WikiLeaks published the messages in a searchable database, similar to the one it created in October for emails alleged to have come from the account of John Podesta, the campaign chair for Democratic presidential nominee Hillary Clinton. The Macron emails were initially published in May, just two days before the French people voted in the presidential election. Macron was seen as a frontrunner against his far-right rival Marine Le Pen. Macron confirmed the hack then, saying in a statement through his political party: "The En Marche! Movement has been the victim of a massive and coordinated hack this evening which has given rise to the diffusion on social media of various internal information." The emails were posted on a profile called EMLEAKS to Pastebin, according to Reuters. It was unclear who was responsible for the leaks, the head of France's cybersecurity agency ANSSI saying in June that "it could be anyone." The leaks proved to have little impact on the French election. Macron beat Le Pen in a landslide. WikiLeaks said its DKIM system is able to sift through the emails to independently to authenticate the content and sender.

Apple kowtows to China, pulls some VPN apps from Chinese App Store

Fox News, 31 Jul 2017: The tech giant's move has sparked criticism from service providers, who say that Virtual Private Networks are crucial for users bypassing the so-called "Great Firewall of China." Over the weekend, Apple was forced to remove the VPN apps from the local version of the App Store after the Chinese government appears to have sent a message on government censorship. When asked for comment by Fox News, an Apple spokesman said: "Earlier this year China's [Ministry of Industry and Information Technology] announced that all developers offering VPNs must obtain a license from the government. We have been required to remove some VPN apps in China that do not meet the new regulations. These apps remain available in all other markets where they do business." VPNs allow Chinese internet users to bypass the country's firewall, using them to circumvent the restrictions China places on foreign websites, as well as hiding internet browsing activity from internet service providers. Websites such as YouTube, Twitter and Facebook are all blocked in China. Several VPN companies knocked the move, saying Apple may not fully realize what it has done by removing these apps. NordVPN is still working in China, but Kamden added that the company never had an Apple app as it was "expecting similar issues." StarVPN, which had its VPN app blocked, tweeted the movie is a "dangerous precedent." China is Apple's third-largest market, behind North America and Europe and the company has been struggling there in recent quarters.

Hackers breach dozens of voting machines brought to conference

TheHill, 29 Jul 2017: One of the nation's largest cybersecurity conferences is inviting attendees to get hands-on experience hacking a slew of voting machines, demonstrating to researchers how easy the process can be. “It took me only a few minutes to see how to hack it,” said security consultant Thomas Richards, glancing at a Premier Election Solutions machine currently in use in Georgia. The DEF CON cybersecurity conference is held annually in Las Vegas. This year, for the first time, the conference is hosting a "Voting Machine Village" where attendees can try to hack a number of systems and help catch vulnerabilities. The conference acquired 30 machines for hackers to toy with. Every voting machine in the village was hacked. Though voting machines are technologically simple, they are difficult for researchers to obtain for independent research. The machine that Richards learned how to hack used beneath-the-surface software, known as firmware, designed in 2007. But a

b6
b7C

[redacted]

[redacted]

This Issue's News Articles:

- Hackers Break Into HBO's Computer Networks, May Have Leaked 'Game of Thrones'
- Facebook shuts down robots after they invent their own language
- WikiLeaks publishes searchable archive of Emmanuel Macron's campaign emails
- FCC says its cybersecurity measures to prevent DDoS attacks must remain secret
- 'Most dangerous' banking trojan gets update
- RNC tells staff not to delete or alter any documents related to 2016 campaign
- Hackers claim 'breach' of cyber firm FireEye
- AI quickly cooks malware that AV software can't spot
- It's 2017 and Hayes AT modem commands can hack luxury cars
- McAfee online scan used plain old HTTP to fetch screen elements

b6
b7C
b7E

Hackers Break Into HBO's Computer Networks, May Have Leaked 'Game of Thrones'

Script Variety, 31 Jul 2017: Hackers have broken into the networks of HBO and reportedly leaked unreleased episodes of a number of shows, as well as the script for next week's "Game of Thrones" episode. Altogether, they have reportedly obtained a total of 1.5 terabyte of data. HBO confirmed the intrusion in a statement sent to Variety: "HBO recently experienced a cyber incident, which resulted in the compromise of proprietary information. We immediately began investigating the incident and are working with law enforcement and outside cybersecurity firms. Data protection is a top priority at HBO, and we take seriously our responsibility to protect the data we hold." Entertainment Weekly was first to report about the hack, and allegedly leaked content, Monday. According to that report, the hackers have already leaked unreleased episodes of "Ballers" and "Room 104." HBO chairman and CEO Richard Plepler addressed the hack in an email to employees, calling it "disruptive, unsettling, and disturbing for all of us." It's still unclear who is behind the hack, but it's far from the first time that Hollywood has found itself in the crosshairs of hackers. A group of hackers that is thought to have been backed by North Korea broke into the networks of Sony Pictures in 2014, and subsequently released tens of thousands of emails as well as scripts and video files. And in late 2016, hackers broke into the network of a small Hollywood-based post-production vendor and stole TV show episodes from Netflix and multiple other TV networks.

b7E

came as the U.S. House passed legislation Tuesday intended to crack down on Russia, as well as North Korea and Iran. The bill is expected to pass the Senate as well, and await President Trump's signature. According to the White House, Trump supports a plan to place sanctions on Russia, though that could interfere with his goal of achieving a better relationship with the country.

The biggest threat to cybersecurity is not enough info sharing

CSO Online, 26 Jul 2017: Even the Department of Defense is working hard to keep pace with the changing landscape of cybersecurity threats. The key, by most estimates, is information sharing. But whether the DOD and other agencies are ready for the level of sharing required is another matter. At the Defensive Cyber Operations Symposium held this past June, Justin Ball, technical director for the Department of Defense Information Network's Operations and Defensive Planning Division, spoke about some of the challenges faced by the agency in the face of new and increased security threats. The Department of Defense Information Network (DoDIN) is a globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating and managing information on-demand to warfighters, policy makers and support personnel. Ball acknowledged that considerable attention has been given recently to the standing up of cyber mission teams in the DOD, and the importance of cyber workforces throughout all levels of government. For these teams and workforces to succeed, however, he noted that threat information must be shared broadly and systematically. A successful cybersecurity program must not only be defensive but offensive, Ball explained. It's important to know against whom you should initiate proactive countermeasures, rather than just reacting to the latest advanced threat. And advanced threats themselves are on the increase, with network compromises more insidious and harder to detect than ever before. One of the lessons driven home after the colossal security breach of the Office of Personnel Management in 2015 was how long it can actually take for a threat to be detected. The average lag time is a shocking 205 days, and even 250 days is not unheard of. Because of the interconnectedness of communications, new mobile vulnerabilities and new malware variants are being continually introduced. It's becoming nearly impossible for any agency to keep up all by itself. Ball used DoDIN as an example. While DoDIN's priority is operations, it is also tasked with "freedom of action" in cyberspace while denying that same freedom to adversaries. System operators must conduct full spectrum cyberspace operations (computer network defense, computer network attack and computer network exploitation.) Cyberspace operations are informed by intel and threat indicators from traditional and advanced sensors, sharing vulnerability information from both DOD and non-DOD sources. DOD is using a variety of systems to gather threat information, Ball said. These include Host Based Security Systems, web content filters, an enterprise email security gateway and the Joint Regional Security Stack for the military's Joint Information Environment. Another tool is SharkSeer, a National Security Agency project that aims to detect and mitigate web-based Zero-Day malware and Advanced Persistent Threats using commercial-off-the-shelf technology. DOD is also using privately sourced threat intel, such as McAfee Global Threat Intelligence; the Red Seal Threat Resource Library; and the Tenable Nessus Scanner and Passive Vulnerability Scanner. While commercial sources of threat identification are important for DOD, so too is threat information shared by America's partners in the so-called Five Eyes intelligence alliance that includes Australia, Canada, New Zealand and the United Kingdom. Ball noted, however, that the agency is behind the curve on information sharing, and is challenged as to how to ingest reporting information. Automated event and incident management tools are where threat feeds really come into play, Ball noted. Analytics is required to process that much information, so automation needs to be a bigger part of any information-sharing regime. Within the DOD, information security and continuous monitoring efforts such as risk scoring help identify "defense in depth" gaps. Defense in depth is the principle of having multiple layers of security mechanisms to increase the security of the system. If attacks cause one mechanism to fail, other layers are in place to protect